Amendments to the Specification

Please replace the paragraph on Page 1, lines 6 - 13, with the following marked-up replacement paragraph:

-- This application is related to the applications having serial numbers 09/416,332 entitled "Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections to a Server with which a Client Shares a Message Encoding Scheme" (now U. S. Patent 6,751,731), 09/415,827 entitled "Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections from a Client to a Server using a Trusted Third Party" (now U. S. Patent 6,775,772), and 09/416,100 09/415,645 entitled " Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections When a Server Will Not Use a Message Encoding Scheme Proposed by a Client" (now U. S. Patent 6,694,431), all assigned to the same assignee and filed concurrently herewith on October 12, 1999. --

Please replace the paragraph that begins on Page 4, line 8 and carries over to Page 5, line 4, with the following marked-up replacement paragraph:

-- In such an environment where data is being transmitted between a client and server while passing through intermediate transcoders or gateways, data security is often a key concern. A client may need to send data to the server that is considered security-sensitive by the client or the server, such as when a person's credit card information is transmitted through a network for use by an electronic shopping application executing on the server. In addition, the content dispatched from the server to the client is often considered security-sensitive. A simple example of this situation is the same electronic shopping application just discussed, where the server may

Serial No. 09/415,645   -2-   Docket RSW9-99-084

transmit an order confirmation to the client that includes the client's credit card information. Many other security-sensitive transmissions exist, such as those that occur when using electronic banking, online stock trading, online bill presentment and payment, etc. The problems that may ensue when sensitive data is exposed to an unintended recipient, such as a computer hacker, can be quite serious. While gateways, and transcoders in particular, may be designed to modify the application content in legitimate ways when forwarding it through the delivery chain, sensitive content at the same time must not be disclosed to such intermediaries. (U. S. Patent Application 09/352,534, now U. S. Patent 6,763,460, which is titled "Method for Transmitting Information Data from a Sender to a Receiver via a Transcoder, Method of Transcoding Information Data, Method for Receiving Transcoded Information Data, Sender, Transcoder and Receiver" and is assigned to the same assignee, defines a novel technique for use in such an environment where the security-sensitive portions of a Hypertext Markup Language, or HTML, document are encrypted while leaving the remaining portions in plain text.) —

Serial No. 09/415,645   -3-   Docket RSW9-99-084